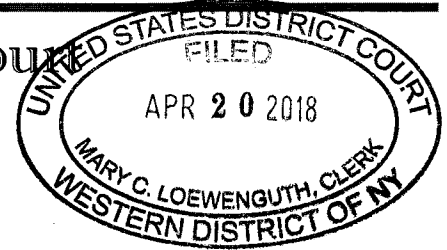


United States District Court
for the
Western District of New York



In the Matter of the Search of

(Briefly describe the property to be searched or identify the person by name and address.)

Email accounts Love2re@mail.com & jaybucci@dr.com,
stored at premises owned, maintained, controlled, or
operated by 1&1 Mail & Media, Inc., a company
located at 701 Lee Road, Suite 300, Chesterbrook, PA 19087,
more further described in Attachment A.

Case No. 18-MJ- 4044

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property located in the Western District of New York (identify the person or describe the property to be searched and give its location): Email accounts Love2re@mail.com & jaybucci@dr.com, stored at premises owned, maintained, controlled, or operated by 1&1 Mail & Media, Inc., a company located at 701 Lee Road, Suite 300, Chesterbrook, PA 19087, more further described in Attachment A.

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

See Attachment B, Schedule of Items to be Seized, which attachment is incorporated by reference as if fully set forth herein, all of which are fruits, evidence and instrumentalities of a violation of Title 18, United States Code, Sections 1030 & 1343.

The basis for search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Title 18, United States Code, Sections 1030 & 1343.

The application is based on these facts: See attached affidavit.

- ☒ continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Meredith McClatchy, S/A FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: April 20, 2018

Judge's signature

City and state: Rochester, New York

Hon. Marian W. Payson, U.S. Magistrate Judge

Printed name and Title

ATTACHMENT A – 1&1
Property to be Searched

This warrant applies to information associated with the following email accounts stored at premises owned, maintained, controlled, or operated by 1&1 Mail & Media, Inc., a company located at 701 Lee Road, Suite 300, Chesterbrook, PA 19087.

- a. Love2re@mail.com
- b. jaybucci@dr.com

ATTACHMENT B – 1&1

I. Information to be Seized

The following procedures shall be implemented in executing the warrant:

1. The warrant will be presented to 1&1, personnel by law enforcement agents. 1&1, personnel will be directed to isolate those accounts and files described below;
2. In order to minimize any disruption of computer service to innocent third parties, the system administrator will create an exact duplicate of the accounts and files described in Attachment A, including an exact duplicate of all information stored in the computer accounts and/or files described below;
3. The 1&1, system administrator will provide the exact duplicate of the accounts and files described below and all information stored in those accounts and /or files to the Special Agent who serves this search warrant;
4. Law enforcement personnel will thereafter review the information stored in the accounts and files received from the system administrator and then identify and copy the information contained in those accounts and files which are authorized to be further copied by this search warrant;
5. Law enforcement personnel will then seal the original duplicate of the accounts and files received from the system administrator and will not further review the original duplicate absent an order of the Court.

II. Information to be disclosed by 1&1

To the extent that the information described in Attachment A is within the possession, custody, or control of 1&1, 1&1, is required to disclose the following information to the government for each account or identifier listed in Attachment A:

1. The contents of all emails stored in the account, including copies of emails sent from the account;
2. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any creditor bank account number);
3. All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;

4. All content in the Docs, Calendar, Friend Contacts and Photos areas;
5. Any and all files linked to email accounts of the user; and
6. All records pertaining to communications between 1&1 and any person regarding the account, including contacts with support services and records of actions taken.

III. Information to be seized by the government

1. All records or information, since December 1, 2017, including the contents of any and all wire and electronic communications, attachments, stored files, print outs, and header information, that contain evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1343 (Wire Fraud) and § 1030 (unauthorized computer access and computer-related fraud).
2. The contents of any communications that contain the true identity and or location of individuals who conspired to violate 18 U.S.C. § 1343 (Wire Fraud) and § 1030 (unauthorized computer access and computer-related fraud), including their names and addresses, and any disposition of the proceeds of violations of 18 U.S.C. § 1343 (Wire Fraud) and § 1030 (unauthorized computer access and computer-related fraud).
3. Records relating to who created, or used the account or identifier.
4. Records identifying accounts held with companies providing Internet access or remote storage of tangible items, documents, data, or storage media.
5. Records since December 1, 2017, including, but not limited to, video files, audio files, images, stored messages, recordings, books, documents, and cached web pages, relating to violations of 18 U.S.C. § 1343 (Wire Fraud) and § 1030 (unauthorized computer access and computer-related fraud).
6. Records since December 1, 2017, reflecting communications with or the existence, identity, travel, or whereabouts of, any individuals who conspired to violate 18 U.S.C. § 1343 (Wire Fraud) and § 1030 (unauthorized computer access and computer-related fraud).

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF
EMAIL ACCOUNT:

jaybucci@dr.com
love2re@mail.com

Case No. 18-mj-4044

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Meredith McClatchy, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been a Special Agent with the Federal Bureau of Investigation (FBI) since June, 2017. I am currently assigned to the Cyber Squad, Buffalo Division, in Rochester, New York. As part of the Cyber Squad, I work on investigations relating to criminal and national security cyber intrusions. I have gained experience through training and everyday work related to these types of investigations. I am familiar with fundamental operations of the internet, hardware, software, and the communication protocols across each. Experience with similar investigations and working with other FBI Special Agents and computer forensic professionals has expanded my knowledge of internet communications and, more specifically, internet-based obfuscation techniques. I have participated in the execution of warrants involving the search and seizure of computers, computer equipment, mobile phones and tablets, and electronically stored information, in conjunction with various criminal investigations.
2. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7); that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 2516.
3. I make this affidavit in support of an application for a search warrant authorizing the search of an email account controlled by the Service Providers known as 1&1 Mail & Media, Inc. ("1&1"), located at 701 Lee Road, Suite 300, Chesterbrook, PA 19087.
4. The email account and the information to be searched are described in the following paragraphs and in Attachments A and B for the Service Provider. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require the Service Providers to disclose to the

government records and other information in its possession pertaining to the subscriber or customer associated with the account, including contents of communications.

5. I respectfully submit that probable cause exists to believe that evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, Section 1343 (wire fraud), and Section 1030 (unauthorized access and computer-related fraud), the TARGET OFFENSES, will be found in the accounts *jaybucci@dr.com* and *love2re@mail.com*.
6. In my training and experience, I have learned that 1&1 is a company that provides web hosting products, domain registration, email solutions, and servers. 1&1 claims to be one of the top five web hosts in the country and provides free Internet electronic mail (email) access to the public. I have learned that opened and unopened email for subscribers, may be located on the computers owned or leased by 1&1. This application for a search warrant seeks authorization solely to search the computer accounts and/or files following the procedures set forth herein.
7. I am familiar with the facts contained in this affidavit based upon my personal involvement in this investigation, information provided by other law enforcement agents, and private companies. Because this affidavit is submitted for the limited purpose of obtaining search warrants, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to search the above referenced facilities.

RELEVANT STATUTES

8. This investigation concerns alleged violations of 18 U.S.C. § 1343 –Wire Fraud and 18 U.S.C § 1030 – Fraud and Related Activity in Connection with a Computer:
9. 18 U.S.C. § 1343 prohibits a person from devising or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme.
10. 18 U.S.C. § 1030 prohibits a person from (a)(2) intentionally accessing a computer without authorization or exceeds authorized access and thereby obtains (C) information from any protected computer.

PROBABLE CAUSE

11. Jones Hospital, located in Wellsville, within the Western District of New York, is an affiliate of the University of Rochester. On December 25, 2017, Jones Hospital was

the victim of a Ransomware attack in which an unknown cyber actor inserted malicious code onto the hospital servers which encrypted all their digital records and prevented hospital staff from accessing any electronic data or patient records. The encryption software contained language which claimed that the cyber actor would provide an encryption key allowing the hospital to recover their digital files upon payment of a ransom.

12. The Ransomware attack was launched from a Jones Hospital server that was exposed to the public internet, herein referred to as the "victim server". The victim server had the IP Address XXX.XXX.174.157.
13. The day after the Ransomware attack, forensic analysis of the victim server was performed by the University of Rochester Information Security Office (ISO). Forensic analysis of the victim server revealed that the cyber actor gained unauthorized access to the victim server using a version of Microsoft's Remote Desktop Protocol (RDP). This software allows a user to remotely access and control a server over a network connection.
14. The cyber actor gained access to the victim server by logging into a specific account, herein referred to as "the account" maintained on the server. The ISO identified this account on the victim server as a test account, which had an easy to guess password. The cyber actor accessed the victim server without authorization by logging into the account, through RDP, between December 13, 2017 and December 15, 2017.
15. The ISO determined that RDP logs for the account were only available dating back to December 15, 2017. Those logs showed that on December 15, 2017 at 10:19AM EST, the account was successfully logged into from IP Address XXX.XXX.252.255.
16. Further forensic analysis of the account by the ISO revealed that the cyber actor, while logged onto the account, also conducted unrelated web browsing activity on December 13, 2017 and December 14, 2017, as shown by the web logs.
17. Analysis of the web logs from December 13, 2017 revealed that the cyber actor purchased round trip plane tickets using www.tripsta.com, an online booking site. Records identified the flights, date of travel, and passengers for this trip. The flights involved travel between Los Angeles California and Montevideo, Uruguay.
18. The weblogs for the account also showed that the cyber actor accessed mail.com, then went back to tripsta.com and entered the email address *mariden4@mail.com* to compete the ticket purchase. Your affiant knows that mail.com is a free email service owned by 1&1 Mail & Media, Inc (1&1).
19. Forensic analysis of the account's web logs from December 13, 2017 also revealed that the cyber actor purchased a Whitepages Premium account. Your affiant knows that

Whitepages is an online directory service containing contact information and public records for over 500 million people. Whitepages Premium accounts allow users to search for an individual's landline numbers, current address, previous cities of residence, relatives, associates, mobile phone numbers, previous street addresses, and full address history. Forensic analysis of the account's web logs from December 14, 2017 provided that the cyber actor conducted searches on www.whitepages.com for several individuals. Based on my experience investigating cybercrimes, online directory services, such as Whitepages, are used to look up information on victim credit card holders in order to complete fraudulent transactions.

20. Subpoena returns for the account *mariden4@mail.com* provided a list of "Forwarding Address" and a list of "Aliases", which contained over two hundred other email addresses. A Forwarding Address is an email address that the subscriber manually sets up to forward mail received by the primary account. An Alias is an email account with the exact same subscriber information and which is created on or around the same time as the primary account. 1&1 was the service provider for all of the email addresses in the Forwarding Address and Aliases list.
21. There was no email content available for the account *mariden4@mail.com*. Your affiant believes this information indicates that the cyber actor intentionally placed a filter in their account settings which automatically forwarded all email addressed to *mariden4@mail.com* to the emails in the Forwarding Address list then automatically deleted them. Thus, emails sent to *mariden4@mail.com* as a part of the scam would not be found in the mailbox of the account.
22. 1&1 provided that the IP Address login history for *mariden4@mail.com* was only retained through December 27, 2017. The IP Address login history for the account *mariden4@mail.com* showed that the account was logged into from IP Address XXX.XXX.252.255 numerous times between December 27, 2017 and January 3, 2018, the same IP Address found in the RDP logs for the account on the victim server.
23. Subpoena returns for the Whitepages premium account purchased on December 13, 2017 identified the subscriber of the account by name and email. It was paid for using a CitiBank Mastercard. The email address associated with this account was in the Forwarding Address List for *mariden4@mail.com*. The IP Address access history for the account showed that the IP Address of the victim server, XXX.XXX.174.157 accessed the account multiple times on December 14, 2017. Shortly thereafter, the real owner of the MasterCard used to open the Whitepages account filed a fraud claim with CitiBank alleging that he did not authorize the purchase. The charge was credited back by the bank.
24. Subpoenaed records from 1&1 identified all of the Forwarding Address email accounts for *mariden4@mail.com*. Of these multiple Forwarding email addresses, all shared the same subscriber information and IP Address login history. One of the Forwarding

Address accounts logged in from IP Address XXX.XXX.252.255 numerous times between December 31, 2017 and January 7, 2018, the same IP Address used in the RDP Ransomware attack referenced above.

25. Another email address linked to this activity was *veronizop@mail.com*. This email was used to purchase airline tickets online between the United States and Australia. Subpoena returns for *veronizop@mail.com* provided that the user of the account logged in from the IP Address XXX.XXX.252.255 numerous times between January 4, 2018 and January 11, 2018, the same IP Address used in the RDP Ransomware attack referenced above. The email address *veronizop@mail.com* was also in the Alias list for *mariden4@mail.com*.
26. Email address *veronizop@mail.com* was also used to book additional airline tickets in January 2018 from IP Address XX.XXX.227.87. The FBI had previously encountered this IP Address in an unrelated investigation in August of 2017 and it was associated with a Dark Web Marketplace that sold RDP logon credentials to compromised servers.
27. The email accounts *mariden4@mail.com*, and *veronizop@mail.com* and their respective Forwarding Address and Aliases lists, all had the same subscriber information and IP Address login history. 1&1 determined that *pauldiren@mail.com* was the master account for the email accounts, and the additional Forwarding Address and Aliases were added from the master account. Additionally, a login to one of the accounts associated with the master account would create a log in record for all other accounts associated with the master account, thus all accounts attached to the master account have the same IP Address login history. There was no email content available for the account *pauldiren@mail.com*. Email accounts could be set to active or inactive. An inactive account could receive email, but automatically pass the email on to the Forwarding Address list, thus acting as an intermediary account.
28. For all of the email accounts operated by *pauldiren@mail.com*, the only emails that were set to active were *jaybucci@dr.com* and *love2re@mail.com*. Both *jaybucci@dr.com* and *love2re@mail.com* had content stored in the accounts. 1&1 determined that *jaybucci@dr.com* was set as the "Default Sender". 1&1 defined the "Default Sender" as the email account through which all outbound communication and content was sent from. 1&1 determined that *love2re@mail.com* was set as the "Default Receiver", and defined the "Default Receiver" as the email account through which all inbound communication was received by. Thus, all incoming and outgoing communication for email the addresses operated by the master account *pauldiren@mail.com* were stored in the accounts *love2re@mail.com* and *jaybucci@dr.com*.
29. Based on my training and experience, and the facts stated above, it is reasonable to believe that the email accounts operated by the master account *pauldiren@mail.com* are operated by the cyber actor who accessed the Jones Hospital server without

authorization from December 13, 2017 to December, 15, 2017. Furthermore, it is reasonable to believe that the cyber actor is accessing servers, without authorization, and using their anonymous status while on the servers to purchase airline tickets and other online subscriptions with unauthorized credit card information.

30. The cyber actor consistently utilized email addresses operated by the master account *pauldiren@mail.com* to facilitate their scheme, as demonstrated by the consistent nature with which he/she provided the captioned email addresses in the contact information for flight tickets and online subscription purchases. Your affiant knows that airlines typically require passengers to provide an email address at the time of ticket purchase. Based on their prior behavior, it is reasonable to believe that the cyber actor has provided email addresses operated by the master account *pauldiren@mail.com* for other flight purchases with unauthorized credit card information.
31. As shown in the subpoena returns for the email accounts operated by master account *pauldiren@mail.com*, the cyber actor conducted email activity on key dates of fraudulent activity associated with this scheme. With the scheme continuing as recent as January 12, 2018, it is reasonable to believe that the cyber actor could have sent or received communications regarding this scam on the *love2re@mail.com* and *jaybucci@dr.com* email accounts.
32. For the purposes of this Search Warrant, the Affiant has only included facts relevant to establish probable cause for this affidavit.
33. Based on my knowledge and experience, as well as the facts previously stated, there is probable cause to believe that the cyber actor who accessed the Jones Hospital server without authorization is in control of the email accounts *love2re@mail.com* and *jaybucci@dr.com*. Further, as the Default Sender and Default Receiver for the master account *pauldiren@mail.com*, there is probable cause to believe the above email accounts were used in facilitation of the TARGET OFFENSES.

DEFINITIONS OF TECHNICAL TERMS USED IN THIS AFFIDAVIT

34. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."
35. I have had training in the investigation of computer-related crimes. Based on my training, and experience, I know the following:
 - a. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the

Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The world wide web ("www") is a functionality of the Internet which allows users of the Internet to share information;

- b. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods; and
 - c. Email is a popular form of transmitting messages and/or files in an electronic environment between computer users. When an individual computer user sends email, it is initiated at the user's computer, transmitted to the subscriber's mail server, then transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An email server may allow users to post and read messages and to communicate via electronic means.
36. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. Many individual computer users and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet email accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP.
37. The ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, email transaction information, posting information, account application information, Internet Protocol addresses, and other information both in computer data format and in written record format.
38. "Internet Protocol address" or "IP address" is a unique numeric address used to identify computers on the Internet. The standard format for IP addressing consists of four numbers between 0 and 255 separated by dots, e.g., 149.101.10.40. Every computer connected to the Internet (or group of computers using the same account to access the Internet) must be assigned an IP address so that Internet traffic, sent from and directed to that computer, is directed properly from its source to its destination. Internet Service Providers (ISPs) assign IP addresses to their customers' computers.

39. "Remote Desktop Protocol" (RDP) is a proprietary protocol which allows a user to remotely connect to another computer via a network connection. The user employs RDP client software for this purpose, which the remote computer must run RDP server software to enable the connection. RDP software clients exist for most versions of Microsoft Windows, Linux, Unix, macOS, iOS, Android, and other operating systems. For example, RDP can be used to access one's work computer from home. While connected, the local user is presented with a graphical interface to the remote machine as well as input capability.
40. The "Dark Web" is the World Wide Web content that exists on overlay networks that use the Internet but require specific software, configurations, or authorization to access. The Dark Web forms a small part of the Deep Web, the part of the Web not indexed by web search engines. A "Dark Web Marketplace" is a commercial website on the Dark Web, functioning primarily as a black market, selling or brokering transactions involving drugs, cyber-arms, weapons, counterfeit currency, stolen credit card details, forged documents, and other illicit goods as well as the sale of legal products.

BACKGROUND REGARDING 1&1

41. 1&1 was the service provider for all of the email addresses in the Forwarding Address and Aliases list referenced within this affidavit. Based on my training and experience, I have learned the following about 1&1:
 - a. 1&1 is one of the world's leading Web hosting providers. 1&1 currently offers a wide range of Web hosting products, including email solutions and high-end servers in 10 different countries including Germany, Spain, Great Britain, and the United States. One aspect of 1&1's business involves providing subscribers with internet-based email.
 - b. 1&1 is considered an electronic communications service ("ECS") provider because it provides its users access to electronic communications service as defined in Title 18, United States Code, Section 2510(15). Internet users sign-up for a subscription for these electronic communication services by registering on the Internet with 1&1. 1&1 requests subscribers to provide basic information, such as name, gender, zip code and other personal/biographical information. However, 1&1 does not verify the information provided. As part of its services, 1&1 also provides its subscribers with the ability to set up email accounts;
 - c. 1&1 maintains electronic records pertaining to the individuals and companies for which they maintain subscriber accounts;

- d. Subscribers to 1&1 may access their accounts on servers maintained or owned by 1&1 from any computer connected to the Internet located anywhere in the world;
- e. Any email that is sent to a 1&1 subscriber is stored in the subscriber's "mail box" on 1&1's servers until the subscriber deletes the email or the subscriber's mailbox exceeds the storage limits preset by the internet service provider. If the message is not deleted by the subscriber, the account is below the storage limit, and the subscriber accesses the account periodically, that message can remain on 1&1's servers indefinitely;
- f. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to 1&1's servers, and then transmitted to its end destination. 1&1 users have the option of saving a copy of the email sent. Unless the sender of the email specifically deletes the email from the 1&1 server, the email can remain on the system indefinitely. The sender can delete the stored email message, thereby eliminating it from the email box maintained at 1&1, but that message will remain in the recipient's email box unless the recipient also deletes it or unless the recipient's account has exceeded its storage limitations;
- g. A 1&1 subscriber can store files, including emails and image files, on servers maintained and/or owned by 1&1; and
- h. Emails and image files stored on a 1&1 server by a subscriber may not necessarily also be located in the subscriber's home computer. The subscriber may store emails and/or other files on the 1&1 server for which there is insufficient storage space in the subscriber's own computer or which the subscriber does not wish to maintain in his or her own computer. A search of the subscriber's home, business, or laptop computer will therefore not necessarily uncover files the subscriber has stored on the 1&1 servers.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

42. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require the Service Providers to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I in the Attachment B annexed hereto. Because the Service Providers are not aware of the facts of this investigation, their employees are not in a position to search for relevant evidence. In addition, requiring the Service Providers to perform the search would be a burden upon the companies. If all the Service Providers were asked to do was produce all the files associated with the account, an employee can do that easily. Requiring the Service Providers to search the materials to determine

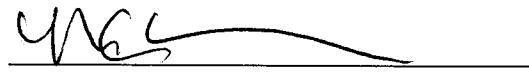
what content is relevant would add to their burden. Upon receipt of the information described in Section I in the Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

43. Based on my training and experience, and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that in the email account located on computer systems owned, maintained, and/or operated by 1&1 Mail & Media, Inc., located at 701 Lee Road, Suite 300, Chesterbrook, PA 19087 there exists evidence, contraband, fruits, and instrumentalities of violations of Title 18 U.S.C. § 1030 (unauthorized computer access and computer-related fraud) and 1343 (Wire Fraud). I therefore respectfully request that the Court issue a search warrant directed to the Service Providers for the email account identified in the Attachment A for information described in the Attachment B.
44. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) and (c)(1)(A). Specifically, the Court is "a district court of the United States ... that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).
45. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING

Because this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto could jeopardize the progress of the investigation. Disclosure of the search warrant at this time could jeopardize the investigation by giving the targets an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee from prosecution. Accordingly, I request that the Court issue an order that the search warrant, this affidavit in support of application for search warrant, the application for search warrant, and all attachments thereto be filed under seal until further order of this Court.


Meredith McClatchy, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
this 20 day of April, 2018


HONORABLE MARIAN W. PAYSON
UNITED STATES MAGISTRATE JUDGE